ASAファイアウォールでのネットワークアドレス変換(NAT)とACLの設定

内容

概要

このドキュメントでは、ASAファイアウォールでネットワークアドレス変換(NAT)とアクセスコントロールリスト(ACL)を設定する方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、ASA コード バージョン 9.1(1) が稼働する ASA 5510 ファイアウォールに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています

。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、アウトバウンド接続とインバウンド接続を許可するためにASAファイアウォールでNATとACLを設定する方法の簡単で簡単な例について説明します。これは、ASAコードバージョン9.1(1)を実行する適応型セキュリティアプライアンス(ASA)5510ファイアウォールで作成されていますが、他のASAファイアウォールプラットフォームにも簡単に適用できます。物理インターフェイスの代わりに VLAN を使用する ASA 5505 などのプラットフォームを使用する場合は、適切なインターフェイス タイプに変更する必要があります。

概要

目標

この設定例では、ASAファイアウォールのDMZ内のWebサーバへのインバウンドアクセスを許可し、内部ホストとDMZホストからのアウトバウンド接続を許可するために必要なNATおよびACLの設定について説明します。これは、次の 2 つの目的に集約できます。

1. 内部および DMZ のホストに、インターネットへの発信接続を許可する。
2. インターネット上のホストが、IPアドレス192.168.1.100のDMZ上のWebサーバにアクセスできるようにします。

この2つの目標を達成するために完了する必要がある手順を実行する前に、このドキュメントでは、新しいバージョンのASAコード（バージョン8.3以降）でACLとNATが動作する方法について簡単に説明します。

アクセス コントロール リストの概要

アクセス コントロール リスト（短縮してアクセス リストまたは ACL）は、ASA ファイアウォールがトラフィックを許可するか拒否するかを決定する方法です。デフォルトでは、低いセキュリティ レベルから高いセキュリティ レベルへのトラフィックの通過は拒否されます。これは、低いセキュリティ インターフェイスに ACL を適用することで上書きできます。また ASA では、デフォルトで高いセキュリティ インターフェイスから低いセキュリティ インターフェイスへのトラフィックが許可されます。この動作も ACL で上書きできます。

ASA コードの以前のバージョン（8.2 以前）では、ASA は着信接続または着信パケットを、最初にパケットの逆変換を行わずにインターフェイスの ACL と比較していました。つまり ACL では、インターフェイスでキャプチャした状態のパケットを許可する必要がありました。バージョン 8.3 以降のコードでは、ASA はインターフェイスの ACL をチェックする前にパケットを逆変換します。つまり、8.3 以降のコード、そしてこのドキュメントでは、ホストの変換された IP ではなく、ホストの実際の IP へのトラフィックが許可されます。

ACLの詳細については、『Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1』の「アクセスルールの設定」セクションを参照してください。

NAT の概要

ASA バージョン 8.3 以降の NAT は 2 種類に分かれ、Auto NAT（Object NAT）と Manual

NAT (Twice NAT) として知られています。1 つめの Object NAT は、ネットワーク オブジェクトの定義の中で設定されます。この例については、この後このドキュメントで説明します。Auto NAT の主な利点の 1 つは、競合を避けるために ASA によって処理するルールの順序が自動的に並べ替えられることです。この方法は NAT の最も簡単な形式ですが、この簡明さによってコンフィギュレーションの詳細度は制限されます。たとえば、2 種類目の NAT である Manual NAT では可能な、パケットの宛先に基づいた変換の決定ができません。Manual NAT は詳細度については優れていますが、正しい動作を得るためには各行を正しい順序で設定する必要があります。これにより、このNATタイプは複雑になるため、この設定例では使用できません。

NATの詳細については、『Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1』の「NATに関する情報」セクションを参照してください。

設定

はじめる

基本的な ASA 設定のセットアップでは、3 つのネットワーク セグメントに接続された 3 つのインターフェイスがあります。ISP ネットワーク セグメントは Ethernet0/0 インターフェイスに接続され、セキュリティ レベル 0 の outside のラベルが付けられます。内部ネットワークは Ethernet0/1 に接続され、セキュリティ レベル 100 の inside のラベルが付けられます。Web サーバが存在する DMZ セグメントは Ethernet0/2 に接続され、セキュリティ レベル 50 の DMZ のラベルが付けられます。

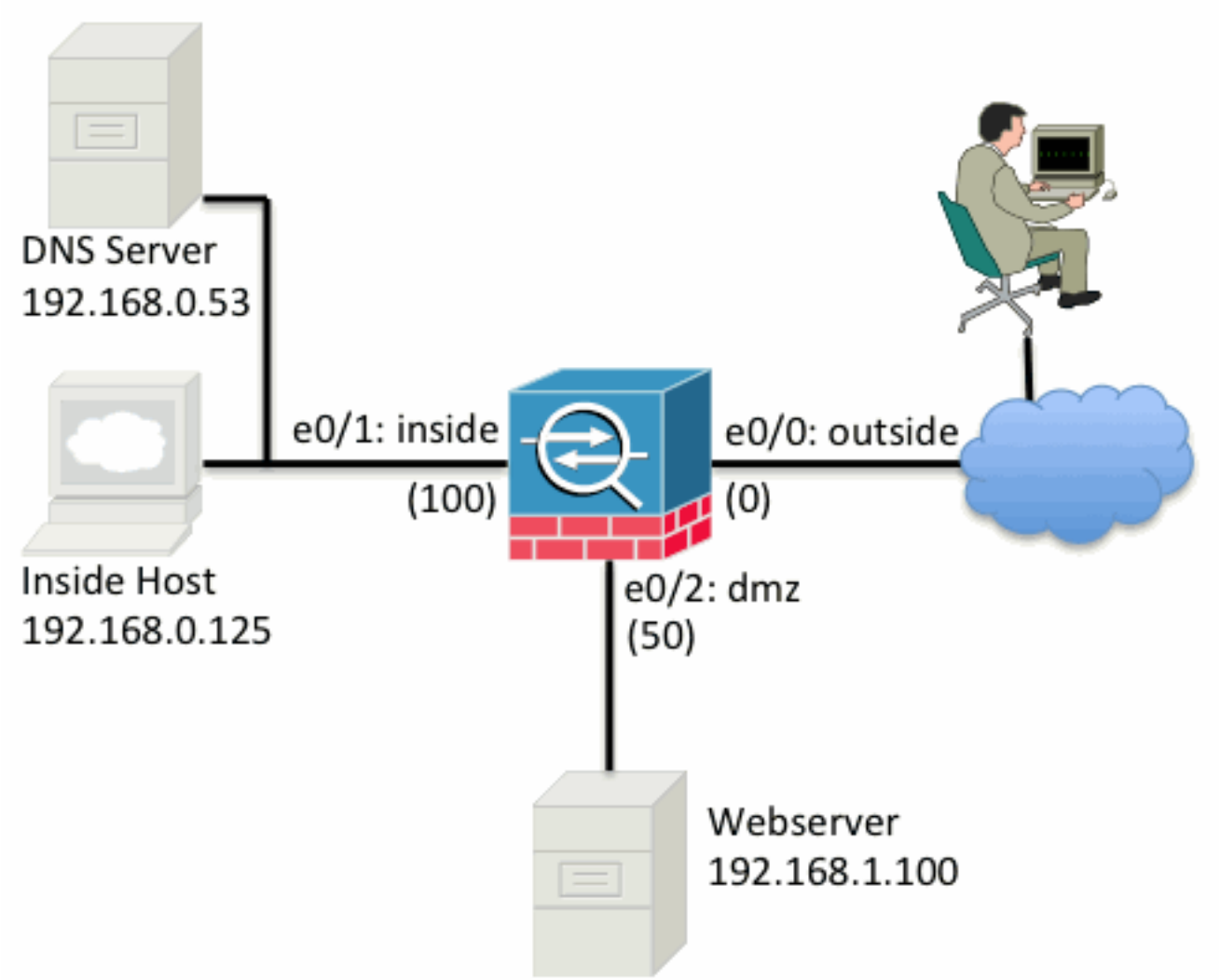
この例のインターフェイスのコンフィギュレーションと IP アドレスは次のようになります。

```
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

ASA の inside インターフェイスは IP アドレスが 192.168.0.1 に設定されていることがわかります。これが内部ホストのデフォルト ゲートウェイです。ASA の outside インターフェイスは ISP から入手した IP アドレスで設定されています。ネクスト ホップを ISP のゲートウェイに設定するデフォルト ルートが設定されています。DHCP を使用する場合、これは自動的に提供されます。DMZ インターフェイスは IP アドレスが 192.168.1.1 に設定されています。これが DMZ ネットワーク セグメント上のホストのデフォルト ゲートウェイです。

トポロジ

ケーブル接続と設定を次に図示します。



ステップ 1：ホストがインターネットにアクセスできるようにNATを設定する

この例では、オブジェクトNAT（別名AutoNAT）が使用されています。最初に設定するのは、inside および dmz セグメント上のホストのインターネットへの接続を許可する NAT ルールです。これらのホストはプライベート IP アドレスを使用するので、これをインターネット上でルーティング可能なアドレスに変換する必要があります。この例では、アドレスが ASA の outside インターフェイスの IP アドレスに見えるように変換します。外部 IP が（おそらく DHCP によって）頻繁に変更される場合、このセットアップはとても簡単です。

この NAT を設定するには、内側のサブネットを表すネットワーク オブジェクトと、dmz のサブネットを表すネットワーク オブジェクトを作成する必要があります。これらの各オブジェクトで、これらのクライアントがそれぞれのインターフェイスから外部インターフェイスに渡されるときにポートアドレス変換(PAT)を実行できるダイナミックNATルールを設定します。

このコンフィギュレーションは次のようになります。

```
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
nat (inside,outside) dynamic interface
!
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
nat (dmz,outside) dynamic interface
```

この時点での実行コンフィギュレーション（show runコマンドの出力を使用）を見ると、オブジ

ェクト定義が出力の2つの部分に分割されていることがわかります。最初の部分ではオブジェクトに含まれる内容 (ホスト/サブネット、IP アドレスなど) のみが示され、2 番目のセクションでは、そのオブジェクトに結び付けられた NAT ルールが表示されます。前の出力で、最初の部分は次のようになっています。

192.168.0.0/24 サブネットと一致するホストが、inside インターフェイスから outside インターフェイスへ通過する場合は、そのホストを動的に outside インターフェイスに変換します。

ステップ 2：インターネットからWebサーバにアクセスするためのNATの設定

inside および DMZ インターフェイスのホストがインターネットに到達できるようになったので、次にインターネット上のユーザが Web サーバの TCP ポート 80 にアクセスできるようにコンフィギュレーションを変更する必要があります。この例では、インターネット上のユーザがISPから提供された別のIPアドレス(*所有する追加のIPアドレス*)に接続できるように設定されています。この例では 198.51.100.101 を使用します。この設定では、インターネット上のユーザはTCPポート80の198.51.100.101にアクセスすることでDMZ Webサーバに到達できます。このタスクにはオブジェクトNATを使用します。ASAはWebサーバ(192.168.1.100)のTCPポート80を外部のTCPポート80の198.51.100.101のように変換できます。同様に、オブジェクトを定義し、オブジェクトの変換ルールを定義します。また、このホストを変換できるIPを表す2番目のオブジェクトを定義します。

このコンフィギュレーションは次のようになります。

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

この例の NAT ルールの内容をまとめると次のようになります。

IP アドレスが 192.168.1.100 と一致する DMZ セグメント上のホストが、TCP ポート 80 (www) を送信元とする接続を確立し、この接続が outside インターフェイスから送信される場合、これを outside インターフェイスの TCP ポート 80 (www) に変換し、IP アドレスを 198.51.100.101 に変換します。

「TCPポート80(www)が送信元」ですが、Webトラフィックの宛先はポート80です。これらの NAT ルールは本質的に双方向であることを理解することが重要です。そのため、文言を反転して言い換えることも可能です。変換した結果はより理解しやすくなります。

外部のホストが宛先TCPポート80(www)で198.51.100.101への接続を確立する場合、宛先IPアドレスを192.168.1.100に変換し、宛先ポートをTCPポート80(www)にしてDMZに送信できます。

このように表現した方がより理解しやすくなります。次に ACL を設定する必要があります。

ステップ 3：ACL の設定

NAT が設定され、今回のコンフィギュレーションの終了に近づきました。ASA の ACL によって次のようなデフォルトのセキュリティ動作を上書きできることを思い出してください。

- 低いセキュリティ インターフェイスから送信されたトラフィックは、高いセキュリティ インターフェイスに到達すると拒否されます。

- 高いセキュリティ インターフェイスから送信されたトラフィックは、低いセキュリティ インターフェイスに到達すると許可されます。

したがって、コンフィギュレーションに ACL を追加しない場合、この例のトラフィックは次のように動作します。

- inside（セキュリティ レベル 100）のホストは DMZ（セキュリティ レベル 50）のホストに接続できます。
- inside（セキュリティ レベル 100）のホストは outside（セキュリティ レベル 0）のホストに接続できます。
- DMZ（セキュリティ レベル 50）のホストは outside（セキュリティ レベル 0）のホストに接続できます。

ただし次のトラフィックは拒否されます。

- outside（セキュリティ レベル 0）のホストは inside（セキュリティ レベル 100）のホストに接続できません。
- outside（セキュリティ レベル 0）のホストは DMZ（セキュリティ レベル 50）のホストに接続できません。
- DMZ（セキュリティ レベル 50）のホストは inside（セキュリティ レベル 100）のホストに接続できません。

現在のコンフィギュレーションでは、outside から DMZ ネットワークへのトラフィックは ASA によって拒否されるため、ステップ 2 で NAT の設定をしたにもかかわらず、インターネット上のユーザは Web サーバに接続できません。このトラフィックを明示的に許可する必要があります。8.3 以降のコードでは、変換された IP ではなくホストの実際の IP を ACL で使用する必要があります。つまり、コンフィギュレーションでは、宛先が 198.51.100.101 のポート 80 のトラフィックではなく、宛先が 192.168.1.100 のトラフィックを許可する必要があります。わかりやすくするために、ステップ2で定義したオブジェクトをこのACLにも使用できます。ACL を作成したら、それを外側のインターフェイスの着信に適用する必要があります。

これらのコンフィギュレーション コマンドは次のようになります。

```
access-list outside_acl extended permit tcp any object webserver eq www
!
access-group outside_acl in interface outside
```

この access-list 行は次を意味します。

Any（任意の場所）から webserver オブジェクト（192.168.1.100）で表されるホストのポート 80 へのトラフィックを許可します。

ここで any キーワードを使用することが重要です。Web サイトに到達するクライアントの送信元 IP アドレスはわからないため、「任意の IP アドレス」を意味する any を指定します。

dmz セグメントから inside ネットワーク セグメントのホスト宛のトラフィックについてはどうすればよいでしょうか。たとえば、inside ネットワークのサーバに接続する必要のあるホストが DMZ 上に存在する場合です。ASA が dmz から inside サーバ宛の特定のトラフィックのみを許可し、それ以外は inside セグメント宛のトラフィックをすべてブロックするにはどうすればよいでしょうか。

この例では、内部ネットワークに IP アドレス 192.168.0.53 の DNS サーバがあり、DNS 解決のために DMZ 上のホストがアクセスする必要があると仮定します。DMZ インターフェイスに着信するトラフィックに対して、前述したデフォルトのセキュリティ動作を ASA が上書きできるよう

に、必要な ACL を作成して DMZ インターフェイスに適用します。

これらのコンフィギュレーション コマンドは次のようになります。

```
object network dns-server
host 192.168.0.53
!
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
access-group dmz_acl in interface dmz
```

この ACL は、DNS サーバの UDP ポート 53 へのトラフィックを単純に許可するよりも複雑です。最初の許可ラインだけであれば、DMZからインターネット上のホストへのすべてのトラフィックがブロックされます。ACL の最後には暗黙の 'deny ip any any' があるためです。この結果、DMZ のホストはインターネットにアクセスすることができなくなります。DMZ から outside へのトラフィックがデフォルトで許可されていても、DMZ インターフェイスに ACL を適用することによって DMZ インターフェイスのデフォルトのセキュリティ動作は無効となるため、インターフェイスの ACL でトラフィックを明示的に許可する必要があります。

ステップ 4：Packet Tracer機能による設定のテスト

コンフィギュレーションが完了したので、動作を確認する必要があります。最も簡単な方法は実際のホストを使用することです（自分が所有するネットワークの場合）。ただし、CLIからこれをテストし、ASAのツールの一部をさらに詳しく調べるには、パケットトレーサを使用してテストを行い、発生した問題をデバッグする可能性があります。

パケット トレーサは、一連のパラメータに基づいてパケットをシミュレーションし、ワイヤから取り出した実際のパケットのようにそのパケットをインターフェイスのデータパスに挿入します。このパケットには、ファイアウォールを通過するパケットに対して実施される数多くのチェックや処理が行われ、パケット トレーサはその結果を記録します。インターネット上のホストに送信しようとしている内部ホストのシミュレーションを行います。このコマンドは、ファイアウォールに次のことを指示します。

inside インターフェイスに到着した、IP アドレス 192.168.0.125 の送信元ポート 12345 から IP アドレス 203.0.113.1 のポート 80 宛の TCP パケットをシミュレートします。

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config: Additional Information:
in 0.0.0.0 0.0.0.0 outside Phase: 3
Type: NAT
```

```
Subtype:
Result: ALLOW
Config:
object network inside-subnet
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

最終結果ではこのトラフィックは許可されます。これはコンフィギュレーションの NAT と ACL チェックを通過したこと、および出力インターフェイス (outside) から送信されたことを意味します。パケットはフェーズ 3 で変換されており、ヒットしたルールがこのフェーズの詳細に表示されていることに注目してください。ホスト 192.168.0.125 はコンフィギュレーションに従って動的に 198.51.100.100 に変換されています。

次に、インターネットからWebサーバへの接続に対して実行します。インターネット上のホストは、外部インターフェイスの198.51.100.101に接続することによってWebサーバにアクセスできることを思い出してください。このコマンドは次のように翻訳できます。

outside インターフェイスに到着した、IP アドレス 192.0.2.123 の送信元ポート 12345 から IP アドレス 198.51.100.101 のポート 80 宛のTCP パケットをシミュレートします。

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
```

```
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

ここでも、結果はパケットが許可されます。ACLはチェックアウトされ、設定は正常に見え、インターネット（外部）上のユーザは外部IPを使用してそのWebサーバにアクセスできます。

確認

検証手順は「ステップ 4：パケット トレーサ機能を使用してコンフィギュレーションをテストする」に含まれています。

トラブルシュート

現在のところ、この設定のトラブルシューティング方法に関する特定の情報はありません。

結論

基本的なNATを行うためのASAの設定は、それほど難しい作業ではありません。このドキュメントの例は、サンプル コンフィギュレーションで使用されている IP アドレスとポートを変更することによって特定のシナリオに適用できます。コンフィギュレーションをまとめると、この例の最終的な ASA の設定は、ASA 5510 に対しては次のようになります。

```
ASA Version 9.1(1)
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
```

```
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

たとえば ASA 5505 であれば、インターフェイスが前の説明と同様に接続されている場合（Ethernet0/0 に接続された outside、Ethernet0/1 に接続された inside、Ethernet0/2 に接続された DMZ）、次のようになります。

```
ASA Version 9.1(1)
!
interface Ethernet0/0
description Connected to Outside Segment
switchport access vlan 2
!
interface Ethernet0/1
description Connected to Inside Segment
switchport access vlan 1
!
interface Ethernet0/2
description Connected to DMZ Segment
switchport access vlan 3
!
interface Vlan2
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
```

```
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53



!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。